Bachelor- oder Masterarbeitsthema

„Side-Channel Attacks and Defenses against Intel SGX“

Intel SGX ist eine Technologie für die vertrauenswürdige Ausführung von Programmcode auf nicht vertrauenswürdigen Systemen. Die Technologie hat in den letzten Jahren viel Aufmerksamkeit aus Industrie und Forschung erfahren. Insbesondere wurden von akademischer Seite eine Reihe von Schwachstellen und Angriffen publiziert, die die Sicherheit von SGX teilweise unterwandern.

Die meisten der Angriffe beruhen auf dem Ausnutzen von Designschwachstellen und Seitenkanälen in Intel-Prozessoren. So erlaubte z.B. der „Foreshadow“-Angriff ein Auslesen von SGX-geschützten Daten ähnlich wie der bekanntere „Meltdown“-Angriff ein Auslesen von Kernel-Daten erlaubte.

In der Abschlussarbeit sollen die bekannten Angriffe auf Intel SGX (und möglicherweise verwandte Technologien von ARM und AMD) zusammengetragen, analysiert und teilweise nachimplementiert werden. Idealerweise sollen im Anschluss auch prototypisch Gegenmaßnahmen in Software entwickelt („Stretch Goal I“) oder neue Angriffsvarianten entwickelt werden („Stretch Goal II“).

Die Arbeit wird von Dr.-Ing. Felix Schuster betreut und von Prof. Thorsten Holz geprüft.

Über Edgeless Systems

Wir sind ein vom BMBF finanziertes Startup und am Lehrstuhl von Prof. Holz beheimatet. Wir entwickeln neuartige Technologien für die nachweisbar sichere Verarbeitung von sensiblen Daten. Dabei bauen wir auf Trusted Execution Environments (TEEs) wie Intel SGX.

Wir haben viel Erfahrung mit TEEs und waren vorher bei Microsoft Research UK und G Data beschäftigt. Unser Mitgründer Felix Schuster ist auch Gründungsmitglied der FluxFingers.

Kontakt

Dr.-Ing. Felix Schuster, felix.schuster@rub.de

https://edgeless.systems/